



# **Lokale Storage-Administratorkonten**

## **ONTAP Technical Reports**

NetApp  
January 23, 2026

This PDF was generated from <https://docs.netapp.com/de-de/ontap-technical-reports/ontap-security-hardening/roles-applications-authentication.html> on January 23, 2026. Always check docs.netapp.com for the latest.

# Inhalt

Lokale Storage-Administratorkonten .....	1
ONTAP-Rollen, -Applikationen und -Authentifizierung .....	1
Rollen .....	1
Anwendungsmethoden .....	5
Authentifizierungsmethoden .....	6
Standard-Administratorkonten .....	7
Lokale Konten auflisten .....	7
Legen Sie das Kennwort für das Diagnosekonto (diag) fest .....	7
Überprüfung durch mehrere Administratoren .....	8
Snapshot wird gesperrt .....	9
Richten Sie den zertifikatbasierten API-Zugriff ein .....	9
ONTAP OAuth 2.0 Token-basierte Authentifizierung für REST-API .....	12
Anmelde- und Kennwortparameter .....	12
Neue lokale Kontofunktionen .....	13
SHA-512-Unterstützung .....	13
Kennwortparameter .....	15

# Lokale Storage-Administratorkonten

## ONTAP-Rollen, -Applikationen und -Authentifizierung

ONTAP bietet sicherheitsbewussten Unternehmen die Möglichkeit, verschiedenen Administratoren anhand verschiedener Anmeldeanwendungen und -Methoden granularen Zugriff zu gewähren. So können Kunden ein datenorientiertes Zero-Trust-Modell aufbauen.

Dies sind die Rollen, die Administratoren von Administratoren und Storage Virtual Machines zur Verfügung stehen. Die Methoden der Anmeldeanwendung und die Methoden der Anmeldeauthentifizierung werden angegeben.

### Rollen

Dank rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) haben Benutzer nur Zugriff auf die Systeme und Optionen, die für ihre Rollen und Funktionen erforderlich sind. Die RBAC-Lösung in ONTAP beschränkt den administrativen Zugriff der Benutzer auf das Niveau, das für ihre Rolle festgelegt wurde. Administratoren können so Benutzer anhand der zugewiesenen Rolle managen. ONTAP bietet mehrere vordefinierte Rollen. Operatoren und Administratoren können benutzerdefinierte Zugriffskontrollrollen erstellen, ändern oder löschen und Kontobeschränkungen für bestimmte Rollen festlegen.

#### Vordefinierte Rollen für Cluster-Administratoren

Diese Rolle...	Verfügt über diese Zugriffsebene...	Zu den folgenden Befehlen oder Befehlsverzeichnissen
<code>admin</code>	Alle	Alle Befehlsverzeichnisse (DEFAULT)
<code>admin-no-fsa</code> (Verfügbar ab ONTAP 9.12.1)	Lese-/Schreibzugriff	<ul style="list-style-type: none"><li>• Alle Befehlsverzeichnisse (DEFAULT)</li><li>• <code>security login rest-role</code></li><li>• <code>security login role</code></li></ul>

Schreibgeschützt	<ul style="list-style-type: none"> <li>• security login rest-role create</li> <li>• security login rest-role delete</li> <li>• security login rest-role modify</li> <li>• security login rest-role show</li> <li>• security login role create</li> <li>• security login role create</li> <li>• security login role delete</li> <li>• security login role modify</li> <li>• security login role show</li> <li>• volume activity-tracking</li> <li>• volume analytics</li> </ul>	Keine
volume file show-disk-usage	autosupport	Alle
<ul style="list-style-type: none"> <li>• set</li> <li>• system node autosupport</li> </ul>	Keine	Alle anderen Befehlsverzeichnisse (DEFAULT)
backup	Alle	vserver services ndmp
Schreibgeschützt	volume	Keine
Alle anderen Befehlsverzeichnisse (DEFAULT)	readonly	Alle

<ul style="list-style-type: none"> <li>• security login password</li> </ul> <p>Nur zur Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen</p> <ul style="list-style-type: none"> <li>• set</li> </ul>	Keine	security
Schreibgeschützt	Alle anderen Befehlsverzeichnisse (DEFAULT)	none



Die autosupport Rolle wird dem vordefinierten autosupport Konto zugewiesen, das von AutoSupport OnDemand verwendet wird. ONTAP verhindert autosupport, dass Sie das Konto ändern oder löschen. ONTAP hindert Sie auch daran, die autosupport Rolle anderen Benutzerkonten zuzuweisen.

### Vordefinierte Rollen für SVM-Administratoren (Storage Virtual Machine

Rollenname	Sorgen
vsadmin	<ul style="list-style-type: none"> <li>• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen</li> <li>• Verwalten von Volumes, mit Ausnahme von Volume-Verschiebungen</li> <li>• Managen von Kontingenten, qtrees, Snapshots und Dateien</li> <li>• LUNs managen</li> <li>• Führen Sie SnapLock-Vorgänge aus, mit Ausnahme von privilegiertem Löschen</li> <li>• Konfigurationsprotokolle: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP</li> <li>• Services konfigurieren: DNS, LDAP und NIS</li> <li>• Überwachen von Jobs</li> <li>• Überwachen von Netzwerkverbindungen und Netzwerkschnittstellen</li> <li>• Monitoring des Systemzustands der SVM</li> </ul>

vsadmin-volume	<ul style="list-style-type: none"> <li>• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen</li> <li>• Verwalten von Volumes, mit Ausnahme von Volume-Verschiebungen</li> <li>• Managen von Kontingenten, qtrees, Snapshots und Dateien</li> <li>• LUNs managen</li> <li>• Konfigurationsprotokolle: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP</li> <li>• Services konfigurieren: DNS, LDAP und NIS</li> <li>• Überwachung der Netzwerkschnittstelle</li> <li>• Monitoring des Systemzustands der SVM</li> </ul>
vsadmin-protocol	<ul style="list-style-type: none"> <li>• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen</li> <li>• Konfigurationsprotokolle: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP</li> <li>• Services konfigurieren: DNS, LDAP und NIS</li> <li>• LUNs managen</li> <li>• Überwachung der Netzwerkschnittstelle</li> <li>• Monitoring des Systemzustands der SVM</li> </ul>
vsadmin-backup	<ul style="list-style-type: none"> <li>• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen</li> <li>• Management von NDMP-Vorgängen</li> <li>• Lese-/Schreibzugriff auf ein wiederhergestelltes Volume erstellen</li> <li>• Management von SnapMirror Beziehungen und Snapshots</li> <li>• Anzeigen von Volumes und Netzwerkinformationen</li> </ul>

vsadmin-snaplock	<ul style="list-style-type: none"> <li>• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen</li> <li>• Verwalten von Volumes, mit Ausnahme von Volume-Verschiebungen</li> <li>• Managen von Kontingenten, qtrees, Snapshots und Dateien</li> <li>• Führen Sie SnapLock-Vorgänge durch, einschließlich privilegiertem Löschen</li> <li>• Protokolle konfigurieren: NFS und SMB</li> <li>• Services konfigurieren: DNS, LDAP und NIS</li> <li>• Überwachen von Jobs</li> <li>• Überwachen von Netzwerkverbindungen und Netzwerkschnittstellen</li> </ul>
vsadmin-readonly	<ul style="list-style-type: none"> <li>• Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen</li> <li>• Monitoring des Systemzustands der SVM</li> <li>• Überwachung der Netzwerkschnittstelle</li> <li>• Zeigen Sie Volumes und LUNs an</li> <li>• Services und Protokolle anzeigen</li> </ul>

## Anwendungsmethoden

Die Anwendungsmethode gibt den Zugriffstyp der Anmeldemethode an. Mögliche Werte sind `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, und `telnet`.

Durch Festlegen dieses Parameters wird `service-processor` dem Benutzer Zugriff auf den Service-Prozessor gewährt. Wenn dieser Parameter auf `service-processor`ist`, muss der ``-authentication-method` Parameter auf `password` festgelegt werden, da der Service Processor nur die Authentifizierung unterstützt `password`. SVM-Benutzerkonten können nicht auf den Service-Prozessor zugreifen. Daher können Operatoren und Administratoren den Parameter nicht verwenden `-vserver`, wenn dieser Parameter auf `eingestellt ist service-processor`.

Um den Zugriff auf das weiter einzuschränken `service-processor`, verwenden Sie den Befehl `system service-processor ssh add-allowed-addresses`. Mit dem Befehl `system service-processor api-service` können die Konfigurationen und Zertifikate aktualisiert werden.

Aus Sicherheitsgründen sind Telnet und Remote Shell (RSH) standardmäßig deaktiviert, da NetApp Secure Shell (SSH) für sicheren Remote-Zugriff empfiehlt. Wenn Telnet oder RSH erforderlich ist oder nur einmalig benötigt wird, müssen diese aktiviert sein.

Mit dem `security protocol modify` Befehl wird die vorhandene Cluster-weite Konfiguration von RSH und Telnet geändert. Aktivieren Sie RSH und Telnet im Cluster, indem Sie das Feld `aktiviert` auf `true` einstellen.

## Authentifizierungsmethoden

Der Parameter für die Authentifizierungsmethode gibt die Authentifizierungsmethode an, die für Anmeldungen verwendet wird.

Authentifizierungsmethode	Beschreibung
cert	SSL-Zertifikatauthentifizierung
community	SNMP-Community-Zeichenfolgen
domain	Active Directory-Authentifizierung
nsswitch	LDAP- oder NIS-Authentifizierung
password	Passwort
publickey	Authentifizierung über öffentlichen Schlüssel
usm	SNMP-Benutzersicherheitsmodell



Die Verwendung von NIS wird aufgrund von Schwachstellen bei der Protokollsicherheit nicht empfohlen.

Ab ONTAP 9.3 steht für lokale SSH-Konten verkettete zwei-Faktor-Authentifizierung mit und als die beiden Authentifizierungsmethoden zur Verfügung `admin publickey password`. Zusätzlich zum Feld im Befehl wurde ein neues Feld mit dem `-authentication-method security login Namen -second -authentication-method` hinzugefügt. Entweder `publickey` oder `password` kann als oder als angegeben werden `-authentication-method -second-authentication-method`. Während der SSH-Authentifizierung erfolgt die Reihenfolge jedoch immer `publickey` mit teilweiser Authentifizierung, gefolgt von der Passwortaufforderung zur vollständigen Authentifizierung.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

Ab ONTAP 9.4 `nsswitch` kann als zweite Authentifizierungsmethode mit verwendet werden `publickey`.

Ab ONTAP 9.12.1 kann FIDO2 auch für die SSH-Authentifizierung über ein YubiKey oder andere mit FIDO2 kompatible Geräte genutzt werden.

Ab ONTAP 9.13.1:

- `domain` Konten können als zweite Authentifizierungsmethode mit verwendet werden `publickey`.
- Time-Based One-time password (`totp`) ist ein temporärer Passcode, der von einem Algorithmus generiert wird, der die aktuelle Tageszeit als einen seiner Authentifizierungsfaktoren für die zweite Authentifizierungsmethode verwendet.
- Public Key Revocation wird mit SSH `publickeys` sowie Zertifikaten unterstützt, die während SSH auf Ablauf/Widerruf überprüft werden.

Weitere Informationen zur Multi-Faktor-Authentifizierung (MFA) für ONTAP System Manager, Active IQ Unified Manager und SSH finden Sie unter "[TR-4647: Multifaktor-Authentifizierung in ONTAP 9](#)".



# Standard-Administratorkonten

Das Administratorkonto sollte eingeschränkt sein, da die Rolle des Administrators Zugriff über alle Anwendungen erhält. Das Diagnose-Konto gewährt Zugriff auf die System-Shell und sollte nur für den technischen Support reserviert werden, um Fehlerbehebungsaufgaben durchzuführen.

Es gibt zwei standardmäßige Administratorkonten: `admin` Und `diag`.

Verwaiste Konten sind ein wichtiger Sicherheitsvektor und führen oft zu Schwachstellen, einschließlich der Eskalation von Berechtigungen. Dabei handelt es sich um unnötige und nicht genutzte Konten, die im Benutzerkonto-Repository verbleiben. Dabei handelt es sich in erster Linie um Standardkonten, die nie verwendet wurden oder für die Passwörter nie aktualisiert oder geändert wurden. Um dieses Problem zu beheben, unterstützt ONTAP das Entfernen und Umbenennen von Konten.



Sie können integrierte Konten nicht entfernen oder umbenennen. Wenn ein Administrator das Konto entfernt, wird das integrierte Konto beim Neustart wiederhergestellt. **NetApp empfiehlt**, nicht benötigte integrierte Konten mit dem Befehl `lock` zu sperren.

Obwohl verwaiste Konten ein erhebliches Sicherheitsrisiko darstellen, **NetApp empfiehlt dringend**, die Auswirkungen des Entferns von Konten aus dem lokalen Kontenspeicher zu testen.

## Lokale Konten auflisten

Führen Sie zum Auflisten der lokalen Konten den Befehl aus `security login show`.

```
cluster1::*> security login show -vserver cluster1
```

```
vserver: cluster1
```

User/Group Name	Application	Authentication		Acct Locked	Is-Nsswitch Group
		Method	Role Name		
admin	console	password	admin	no	no
admin	http	password	admin	no	no
admin	ontapi	password	admin	no	no
admin	service-processor	password	admin	no	no
admin	ssh	password	admin	no	no
autosupport	console	password	autosupport	no	no

6 entries were displayed.

## Legen Sie das Kennwort für das Diagnosekonto (diag) fest

Ein Diagnosekonto mit dem Namen `diag` wird im Lieferumfang des Speichersystems angegeben. Sie können das Konto verwenden `diag`, um Fehlerbehebungsaufgaben im durchzuführen `systemshell`. Das `diag` Konto ist das einzige Konto, mit dem über den privilegierten Befehl auf die Systemshell zugegriffen werden kann `diag systemshell`.



Die Systemshell und das zugehörige `diag` Konto sind für Low-Level-Diagnosezwecke vorgesehen. Ihr Zugriff erfordert die Berechtigungsebene für die Diagnose und darf nur unter Anleitung des technischen Supports verwendet werden, um Fehlerbehebungsaufgaben durchzuführen. Weder `diag` das Konto noch das `systemshell` sind für allgemeine administrative Zwecke bestimmt.

### Bevor Sie beginnen

Bevor Sie auf den zugreifen `systemshell`, müssen Sie das Kontokennwort mit dem Befehl festlegen `diag security login password`. Verwenden Sie strenge Passwort-Prinzipien und ändern Sie das `diag` Passwort in regelmäßigen Abständen.

### Schritte

1. Legen Sie das Kennwort für den Kontobenutzer fest `diag` :

```
cluster1::> set -privilege diag
```

```
Warning: These diagnostic commands are for use by NetApp personnel only.  
Do you want to continue? \{y|n\}: y
```

```
cluster1::*> systemshell -node node-01  
      (system node systemshell)  
diag@node-01's password:
```

```
Warning: The system shell provides access to low-level  
diagnostic tools that can cause irreparable damage to  
the system if not used properly. Use this environment  
only when directed to do so by support personnel.
```

```
node-01%
```

## Überprüfung durch mehrere Administratoren

Ab ONTAP 9.11.1 können Sie mithilfe von MAV (Multi-Admin Verification) bestimmte Vorgänge, wie das Löschen von Volumes oder Snapshots, nur nach Genehmigungen von designierten Administratoren ausführen lassen. So werden gefährdete, böswillige oder unerfahrene Administratoren daran gehindert, unerwünschte Änderungen vorzunehmen oder Daten zu löschen.

Die Konfiguration der MAV besteht aus folgenden Komponenten:

- "Erstellen einer oder mehrerer Administratorgenehmigungsgruppen".
- "Aktivieren der Funktion zur Verifizierung durch mehrere Administratoren".
- "Hinzufügen oder Ändern von Regeln".

Nach der Erstkonfiguration können nur Administratoren einer MAV-Genehmigungsgruppe (MAV-Administratoren) diese Elemente ändern.

Wenn MAV aktiviert ist, sind für jeden geschützten Vorgang drei Schritte erforderlich:

1. Wenn ein Benutzer den Vorgang initiiert, wird ein ["Die Anforderung wird generiert"](#).
2. Bevor es ausgeführt werden kann, die erforderliche Anzahl von ["MAV-Administratoren müssen genehmigen"](#).
3. Nach der Genehmigung schließt der Benutzer den Vorgang ab.

MAV ist nicht für den Einsatz bei Volumes oder Workflows mit hoher Automatisierung vorgesehen, da jede automatisierte Aufgabe vor Abschluss des Vorgangs eine Genehmigung erfordert. Wenn Sie Automatisierung und MAV gemeinsam nutzen möchten, empfiehlt NetApp, Abfragen für bestimmte MAV-Vorgänge zu verwenden. Sie können beispielsweise MAV-Regeln nur auf Volumes anwenden `volume delete`, auf die keine Automatisierung involviert ist. Sie können diese Volumes einem bestimmten Benennungsschema zuweisen.

Weitere Informationen zum MAV finden Sie im ["Dokumentation zur Verifizierung durch mehrere ONTAP Administratoren"](#).

## Snapshot wird gesperrt

Beim Snapshot-Sperren handelt es sich um eine SnapLock-Funktion, bei der Snapshots manuell oder automatisch mit einer Aufbewahrungsfrist auf der Snapshot-Richtlinie des Volumes unlöschbar gemacht werden. Mit dem Zweck der Snapshot-Sperrung können Sie verhindern, dass abnormale oder nicht vertrauenswürdige Administratoren Snapshots auf dem primären oder sekundären ONTAP System löschen.

Die Snapshot-Sperrung wurde im ONTAP 9.12.1 eingeführt. Snapshot-Sperrung wird auch als manipulationssichere Snapshot Sperrung bezeichnet. Obwohl es die SnapLock-Lizenz und die Initialisierung der Compliance-Uhr erfordert, ist die Snapshot-Sperrung nicht mit SnapLock Compliance oder SnapLock Enterprise verbunden. Es gibt keinen vertrauenswürdigen Storage-Administrator, wie bei SnapLock Enterprise und er schützt nicht die zugrunde liegende physische Storage-Infrastruktur, wie bei der SnapLock Compliance. Dies ist eine Verbesserung gegenüber der SnapVaulting Snapshots auf ein sekundäres System. Die schnelle Recovery von gesperrten Snapshots auf Primärsystemen kann ermöglicht werden, um Volumes wiederherzustellen, die durch Ransomware beschädigt sind.

Weitere Informationen finden Sie im ["Dokumentation zum Sperren von snapshots"](#).

## Richten Sie den zertifikatbasierten API-Zugriff ein

Statt der Benutzer-ID- und Kennwortauthentifizierung für den REST-API- oder NetApp Manageability SDK-Zugriff auf ONTAP muss die zertifikatbasierte Authentifizierung verwendet werden.



Als Alternative zur zertifikatbasierten Authentifizierung für REST-API verwenden Sie ["OAuth 2.0 Token-basierte Authentifizierung"](#).)

Sie können ein selbstsigniertes Zertifikat auf ONTAP erstellen und installieren, wie in den folgenden Schritten beschrieben.

### Schritte

1. Erstellen Sie mithilfe von OpenSSL ein Zertifikat, indem Sie den folgenden Befehl ausführen:

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key  
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"  
Generating a 2048 bit RSA private key  
.....+++  
.....+++  
writing new private key to 'test.key'
```

Dieser Befehl erzeugt ein öffentliches Zertifikat mit dem Namen `test.pem` und einen privaten Schlüssel mit dem Namen `key.out`. Der allgemeine Name `CN` entspricht der ONTAP-Benutzer-ID.

2. Installieren Sie den Inhalt des öffentlichen Zertifikats im Format Privacy Enhanced Mail (pem) in ONTAP, indem Sie den folgenden Befehl ausführen und den Inhalt des Zertifikats einfügen, wenn Sie dazu aufgefordert werden:

```
security certificate install -type client-ca -vserver cluster1  
  
Please enter Certificate: Press <Enter> when done
```

3. Aktivieren Sie ONTAP, um den Clientzugriff über SSL zu erlauben, und definieren Sie die Benutzer-ID für den API-Zugriff.

```
security ssl modify -vserver cluster1 -client-enabled true  
security login create -user-or-group-name cert_user -application ontapi  
-authmethod cert -role admin -vserver cluster1
```

Im folgenden Beispiel ist die Benutzer-ID `cert_user` nun für die Verwendung des zertifikatauthentifizierten API-Zugriffs aktiviert. Ein einfaches Manageability SDK Python-Skript, das zur Anzeige der ONTAP-Version verwendet `cert_user` wird, wird wie folgt angezeigt:

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

Die Ausgabe des Skripts zeigt die ONTAP-Version an.

```
./version.py
```

```
V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. Führen Sie folgende Schritte durch, um eine zertifikatbasierte Authentifizierung mit der ONTAP REST API durchzuführen:

a. Definieren Sie in ONTAP die Benutzer-ID für HTTP-Zugriff:

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

- b. Führen Sie auf Ihrem Linux-Client den folgenden Befehl aus, der die ONTAP-Version als Ausgabe erzeugt:

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key ./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
  "version": {
    "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
    "generation": 9,
    "major": 7,
    "minor": 0
  },
  "_links": {
    "self": {
      "href": "/api/cluster"
    }
  }
}
```

#### Weitere Informationen

- ["Zertifikatbasierte Authentifizierung mit dem NetApp Manageability SDK für ONTAP"](#).

## ONTAP OAuth 2.0 Token-basierte Authentifizierung für REST-API

Als Alternative zur zertifikatbasierten Authentifizierung können Sie die auf OAuth 2.0 Token-basierte Authentifizierung für REST-API verwenden.

Ab ONTAP 9.14.1 haben Sie die Möglichkeit, den Zugriff auf Ihre ONTAP-Cluster über das Open Authorization (OAuth 2.0)-Framework zu steuern. Sie können diese Funktion über jede der ONTAP-Administrationsschnittstellen konfigurieren, einschließlich der ONTAP-CLI, System Manager und REST-API. Die OAuth 2.0-Autorisierungs- und Zugriffskontrollentscheidungen können jedoch nur angewendet werden, wenn ein Client über die REST-API auf ONTAP zugreift.

OAuth 2.0-Token ersetzen Passwörter für die Benutzerkontoauthentifizierung.

Weitere Informationen zur Verwendung von OAuth 2.0 finden Sie im ["ONTAP-Dokumentation zur Authentifizierung und Autorisierung mit OAuth 2.0"](#).

## Anmelde- und Kennwortparameter

Eine effektive Sicherheitslage hält die festgelegten Unternehmensrichtlinien, Richtlinien und alle Governance- oder Standards ein, die für das Unternehmen gelten. Beispiele für diese Anforderungen sind die Lebensdauer des Benutzernamens, Anforderungen an die Länge des Passworts, Zeichenanforderungen und die Speicherung solcher Konten. Die ONTAP-Lösung bietet Funktionen für diese Sicherheitsstrukturen.

## Neue lokale Kontofunktionen

Zur Unterstützung der Richtlinien, Richtlinien oder Standards für Benutzerkonten eines Unternehmens, einschließlich Governance, wird in ONTAP die folgende Funktionalität unterstützt:

- Konfigurieren von Passwortrichtlinien zur Durchsetzung einer Mindestanzahl von Ziffern, Kleinbuchstaben oder Großbuchstaben
- Nach einem fehlgeschlagenen Anmeldeversuch ist eine Verzögerung erforderlich
- Definition des inaktiven Kontonormienlimits
- Ablaufen eines Benutzerkontos
- Eine Warnmeldung zum Ablauf des Kennworts wird angezeigt
- Benachrichtigung über eine ungültige Anmeldung



Konfigurierbare Einstellungen werden über den Befehl `Security Login role config modify` verwaltet.

## SHA-512-Unterstützung

Um die Passwortsicherheit zu verbessern, unterstützt ONTAP 9 die SHA-2-Passwort-Hash-Funktion und verwendet standardmäßig SHA-512, um neu erstellte oder geänderte Passwörter zu hashen. Operatoren und Administratoren können Konten auch nach Bedarf ablaufen lassen oder sperren.

Bereits vorhandene ONTAP 9-Benutzerkonten mit unveränderten Kennwörtern verwenden nach dem Upgrade auf ONTAP 9.0 oder höher weiterhin die MD5-Hash-Funktion. NetApp empfiehlt jedoch dringend, dass diese Benutzerkonten auf die sicherere SHA-512-Lösung migriert werden, indem Benutzer ihre Passwörter ändern müssen.

Mit der Passwort-Hash-Funktion können Sie die folgenden Aufgaben ausführen:

- Benutzerkonten anzeigen, die mit der angegebenen Hash-Funktion übereinstimmen:

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver user-or-group-name application authentication-method hash-
function
-----
-----
cluster1 NewAdmin console password sha512
cluster1 NewAdmin ontapi password sha512
cluster1 NewAdmin ssh password sha512
```

- Konten ablaufen lassen, die eine bestimmte Hash-Funktion (z. B. MD5) verwenden, wodurch Benutzer bei der nächsten Anmeldung gezwungen werden, ihr Passwort zu ändern:

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- Sperren Sie Konten mit Kennwörtern, die die angegebene Hash-Funktion verwenden.

```
cluster1::*> security login lock -vserver * -username * -hash-function md5
```

Die Passwort-Hash-Funktion ist für den internen Benutzer in der Administrations-SVM des Clusters unbekannt `autosupport`. Dieses Problem ist kosmetisch. Die Hash-Funktion ist unbekannt, da dieser interne Benutzer standardmäßig kein konfiguriertes Passwort hat.

- Um die Passwort-Hash-Funktion für den Benutzer anzuzeigen `autosupport`, führen Sie die folgenden Befehle aus:

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

Vserver: cluster1
User Name or Group Name: autosupport
Application: console
Authentication Method: password
Remote Switch IP Address: -
Role Name: autosupport
Account Locked: no
Comment Text: -
Whether Ns-switch Group: no
Password Hash Function: unknown
Second Authentication Method2: none
```

- Um die Passwort-Hash-Funktion (Standard: sha512) einzustellen, führen Sie den folgenden Befehl aus:

```
::> security login password -username autosupport
```

Es spielt keine Rolle, auf welche Art das Passwort eingestellt ist.



```
security login show -user-or-group-name autosupport -instance
```

```
Vserver: cluster1
User Name or Group Name: autosupport
Application: console
Authentication Method: password
Remote Switch IP Address: -
Role Name: autosupport
Account Locked: no
Comment Text: -
Whether Ns-switch Group: no
Password Hash Function: sha512
Second Authentication Method2: none
```

## Kennwortparameter

Die ONTAP Lösung unterstützt Kennwortparameter, die die Anforderungen und Richtlinien des Unternehmens erfüllen und unterstützen.

Ab 9.14.1 gibt es eine erhöhte Komplexität und Sperrregeln für Passwörter, die nur für Neuinstallationen von ONTAP gelten.

Alle Passwörter müssen vom Benutzernamen abweichen.

Attribut	Beschreibung	Standard	Bereich
username-minlength	Mindestlänge des Benutzernamens erforderlich	3	3-16
username-alphanum	Benutzername alphanumerisch	Deaktiviert	Aktiviert/deaktiviert
passwd-minlength	Mindestlänge des Passworts erforderlich	8	3-64
passwd-alphanum	Alphanumerisches Passwort	Aktiviert	Aktiviert/deaktiviert
passwd-min-special-chars	Mindestanzahl an Sonderzeichen im Passwort erforderlich	0	0-64
passwd-expiry-time	Passwortablaufzeit (in Tagen)	Unbegrenzt, d. h. die Passwörter laufen nie ab	0-unbegrenzt 0 == Jetzt ablaufen lassen

Attribut	Beschreibung	Standard	Bereich
require-initial-passwd-update	Erste Kennwortaktualisierung bei der ersten Anmeldung erforderlich	Deaktiviert	Aktiviert/deaktiviert  Änderungen sind über Konsole oder SSH zulässig
max-failed-login-attempts	Maximale Anzahl fehlgeschlagener Versuche	0, Konto nicht sperren	-
lockout-duration	Maximale Sperrzeit (in Tagen)	Der Standardwert ist 0, was bedeutet, dass das Konto für einen Tag gesperrt ist	-
disallowed-reuse	Letzte N-Kennwörter nicht zulassen	6	Der Mindestwert beträgt 6
change-delay	Verzögerung zwischen Passwortänderungen (in Tagen)	0	-
delay-after-failed-login	Verzögerung nach jedem fehlgeschlagenen Anmeldeversuch (in Sekunden)	4	-
passwd-min-lowercase-chars	Mindestanzahl an Kleinbuchstaben im Passwort erforderlich	0. Dies erfordert keine Kleinbuchstaben	0-64
passwd-min-uppercase-chars	Mindestanzahl an alphabetischen Großbuchstaben erforderlich	0. Dies erfordert keine Großbuchstaben	0-64
passwd-min-digits	Mindestanzahl an Ziffern im Passwort erforderlich	0, die keine Ziffern erfordert	0-64
passwd-expiry-warn-time	Warnmeldung vor Ablauf des Passworts anzeigen (in Tagen)	Unbegrenzt, was bedeutet, dass Sie nie vor Ablauf des Passworts warnen	0. Dies bedeutet, dass der Benutzer bei jeder erfolgreichen Anmeldung über den Ablauf des Passworts informiert wird
account-expiry-time	Konto läuft in N Tagen ab	Unbegrenzt, d. h. die Konten laufen nie ab	Die Verfallszeit des Kontos muss größer sein als das Limit für inaktive Konten
account-inactive-limit	Maximale Dauer der Inaktivität vor Ablauf des Kontos (in Tagen)	Unbegrenzt. Das bedeutet, dass die inaktiven Konten nie ablaufen	Das Limit für inaktive Konten muss kleiner als die Ablaufdatum des Kontos sein

## Beispiel

```
cluster1::*> security login role config show -vserver cluster1 -role admin

Vserver: cluster1
Role Name: admin
Minimum Username Length Required: 3
Username Alpha-Numeric: disabled
Minimum Password Length Required: 8
Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
Password Expires In (Days): unlimited
Require Initial Password Update on First Login: disabled
Maximum Number of Failed Attempts: 0
Maximum Lockout Period (Days): 0
Disallow Last 'N' Passwords: 6
Delay Between Password Changes (Days): 0
Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

## Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.